



On the 2024 audit committee agenda

KPMG Board Leadership Center



March 22, 2024

The business and risk environment has changed dramatically over the past year, with greater geopolitical instability, surging inflation, high interest rates, and unprecedented levels of disruption.


Audit committees can expect their company’s financial reporting, compliance, risk, and internal control environment to be put to the test by an array of challenges—from global economic volatility and the wars in Ukraine and the Middle East to cybersecurity risks and ransomware attacks and preparations for global climate and sustainability reporting requirements, which will require developing related internal controls and disclosure controls and procedures.




Drawing on insights from our interactions with audit committees and business leaders, we highlight eight issues to keep in mind as audit committees consider and carry out their 2024 agendas:


 **Stay focused on financial reporting and related internal control risks—job number one.**

 **Focus on leadership and talent in the finance organisation.**

 **Clarify the roles of management’s disclosure committee and ESG teams and committees in preparations for global climate and other sustainability disclosures—and oversee the quality and reliability of the underlying data.**

 **Reinforce audit quality and stay abreast of the increasing expectations of the Accounting and Financial Reporting Council (AFRC)**

 **Maintain focus on cybersecurity and data privacy.**

 **Make sure internal audit is focused on the company’s key risks—beyond financial reporting and compliance—and is a valued resource to the audit committee.**

 **Define the audit committee’s oversight responsibilities for generative artificial intelligence (AI).**

 **Help sharpen the company’s focus on ethics, compliance, and culture.**



Stay focused on financial reporting and related internal control risks—job number one.

Focusing on the financial reporting, accounting, and disclosure obligations posed by the current geopolitical, macroeconomic, and risk landscape will be a top priority and major undertaking for audit committees in 2024.

Forecasting and disclosures. Among the matters requiring the audit committee’s attention are disclosures regarding the impact of the wars in Ukraine and the Middle East, government sanctions, supply chain disruptions, heightened cybersecurity risk, inflation, interest rates, market volatility, and the risk of a global recession; preparation of forward-looking cash-flow estimates; impairment of nonfinancial assets, including goodwill and other intangible assets; impact of events and trends on liquidity; accounting for financial assets (fair value); going concern; and use of non-GAAP metrics. With companies making more tough calls in the current environment, regulators are emphasising the importance of well-reasoned judgments and transparency, including contemporaneous documentation to demonstrate that the company applied a rigorous process. Given the fluid nature of the long-term environment, disclosure of changes in judgments, estimates, and controls may be required more frequently.

Internal control and risk management. Is the audit committee—with management—regularly taking a fresh look at the company’s control environment? While the Corporate Governance Code stipulates a particular role for the audit committee to play in respect of internal controls, the directors of a listed issuer remain collectively and individually responsible for ensuring that internal controls are appropriate and effective. Directors are expected to understand, support and oversee the audit committee’s work, take an active interest in potential deficiencies and assist in implementing any necessary enhancements even if the audit committee is to take a lead role in internal controls¹.

Have controls kept pace with the company’s operations, business model, and changing risk profile, including cybersecurity risks? It is insufficient for a listed issuer to take a passive approach in reviewing and monitoring its internal controls. Internal controls should be considered on an ongoing basis to ensure they remain fit for purpose by design and are fully implemented and working effectively¹.

Committee bandwidth and skill sets. If the company establishes an ESG committee, the audit committee should assume the role of overseeing management’s readiness for global climate and

other sustainability reporting mandates. This extension of the audit committee’s oversight duties goes beyond its foundational responsibilities (financial reporting and related internal controls, and internal and external auditors). The expansion should heighten concerns about audit committee bandwidth and “agenda overload.” Reassess whether the committee has the time and expertise to oversee the major risks on its plate. Such a reassessment is sometimes done in connection with an overall reassessment of issues assigned to each board standing committee. For example, do cybersecurity, climate, sustainability, or “mission-critical” risks such as safety, as well as AI, including generative AI, require more attention at the full board level—or perhaps the focus of a separate board committee? The pros and cons of creating an additional committee should be weighed carefully, but considering whether a finance, technology, risk, climate and sustainability, or other committee—and perhaps the need for directors with new skill sets—would improve the board’s effectiveness can be a healthy part of the risk oversight discussion.

Reassess whether the audit committee has the time and expertise to oversee the major risks on its plate today.



Clarify the roles of management’s disclosure committee and ESG teams and committees in preparations for global climate and other sustainability disclosures—and oversee the quality and reliability of the underlying data.



As discussed in [On the 2024 board agenda](#), an important area of board focus and oversight will be management’s efforts to prepare for global regulatory mandates that will dramatically increase climate and other sustainability disclosure requirements.

Companies with international operations are assessing the potential impacts of, and preparing for compliance with, various ESG regulations. While US companies await final SEC climate rules, they are preparing to comply with [California climate legislation](#) signed into law in October 2023. Those with international operations are assessing the potential impacts of European Sustainability Reporting Standards (ESRSs) issued under the EU’s Corporate Sustainability Reporting Directive (CSRD)—which covers a broad range of sustainability issues beyond climate—and IFRS® Sustainability Disclosure Standards issued by the International Sustainability Standards Board (ISSB), as well

as other foreign disclosure regimes. Countries are already announcing adoption of, or commitments to consider adopting, the final ISSB standards, including Australia (climate only), Brazil, Japan, and the UK.

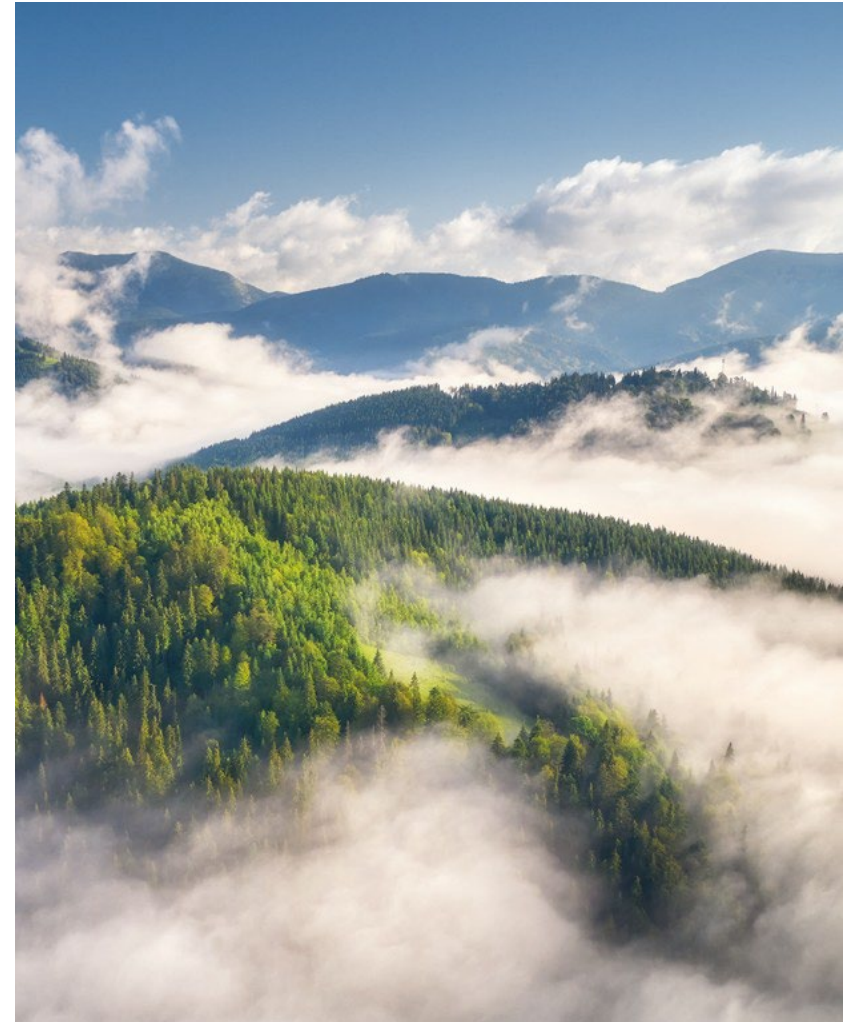
In April 2023, The Stock Exchange of Hong Kong Limited (the Exchange) released a consultation paper proposing enhancements to climate-related disclosures within its ESG framework. These enhancements align with the exposure draft of the IFRS S2 Climate-related Disclosures (ISSB Climate Standard) and their subsequent deliberations ². The initial proposed date for implementation was 1 January 2024. However, the Exchange plans to consider the ISSB Adoption Guide’s recommended scaling and phasing-in of requirements. As a result, the implementation of the Listing Rule amendments will be postponed to 1 January 2025.

Compliance with ESG regulations will be a major undertaking, with cross-functional management teams involved, including management’s disclosure committee and management’s ESG committee—often led by an ESG controller at larger companies—with multiple board committees overseeing different aspects of these efforts. Given the scope of the effort, audit committees should encourage management’s disclosure committee and management’s ESG committee to prepare now by developing management’s path to compliance with applicable reporting standards and requirements—including management’s plan to develop high-quality, reliable climate and sustainability data.

² UPDATE ON CONSULTATION ON ENHANCEMENT OF CLIMATE DISCLOSURES UNDER ESG FRAMEWORK”, the Exchange, 3 November 2023

Key areas of an audit committee focus should include:

- Clarifying the disclosure committee’s role and responsibilities in connection with disclosures contained in regulatory filings and those made voluntarily in sustainability reports, websites, etc., including coordination with cross-functional management ESG committee(s). Since disclosures that are not filed still carry potential liability, management should have processes in place to review these disclosures, including for consistency with filed disclosures.
- Reassessing the composition of the disclosure committee. Given the global climate and other sustainability reporting requirements and the intense focus on these disclosures generally, companies should consider expanding management’s disclosure committee or creating a subcommittee to include appropriate climate and other sustainability functional leaders, such as the ESG controller (if any), chief sustainability officer, chief human resources officer, chief diversity officer, chief supply chain officer, and chief information security officer.
- Encouraging management’s disclosure committee to work with management’s ESG team/committee to identify gaps, consider how to gather and maintain quality information, and closely monitor global rulemaking activities.
- Understanding whether appropriate systems are in place or are being developed to ensure the quality of data that must be assured by third parties.





Maintain focus on cybersecurity and data privacy.

Cybersecurity risk continues to intensify. The acceleration of AI, the increasing sophistication of attacks, the wars in Ukraine and the Middle East, and ill-defined lines of responsibility – among users, companies, vendors, and government agencies – have elevated cybersecurity risk and its place on board and committee agendas.

The growing sophistication of the cyber threat points to the continued cybersecurity challenge – and the need for management teams and boards to continue to focus on resilience. Breaches and cyber incidents are going to happen, and organisations must be prepared to respond appropriately when they do. In other words, it’s not a matter of if, but when.

Regulators and investors are demanding transparency into how companies are assessing and managing cyber risk and building and maintaining resilience.

While data governance overlaps with cybersecurity, it’s broader and includes compliance with industry-specific laws and regulations, as well as privacy laws and regulations that govern how personal data – from customers, employees, or vendors – is processed, stored, collected, and used. Data governance also includes policies and protocols

regarding data ethics – in particular, managing the tension between how the company may use customer data in a legally permissible way and customer expectations as to how their data will be used.

In September 2022, the Chinese Mainland put into effect Measures for the Security Assessment of Cross-Border Data Transfer, and in June 2023, it introduced the Measures for the Standard Contract for the Outbound Transfer of Personal Information³. Banks and other entities engaged in cross-border data transfers must evaluate whether they meet the criteria set by the Cyberspace Administration of China (CAC) and determine the appropriate framework for managing such transfers.

The Office of the Privacy Commissioner for Personal Data (PCPD) in Hong Kong reminds all organisations to adhere to the stipulations under the Personal Data (Privacy) Ordinance (PDPO). This ordinance mandates data users to take all practical steps to protect personal data from unauthorised or accidental access, processing, erasure, loss, or use⁴. Furthermore, organisations are urged to implement preventive measures, heighten their cybersecurity awareness, and regularly review their data security systems.

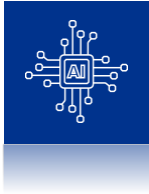
Managing customer data in a legally permissible way and in line with customer expectations poses significant reputation and trust risks for companies and represents a critical challenge for leadership. How robust and up to date is management’s data governance framework? Does it address third-party cybersecurity and data governance risks?

Cyber threats should be considered as part of the company’s risk management process, and the audit committee should test whether the company has:

- Identified the critical information assets which it wishes to protect against cyber attack – the crown jewels of the firm – whether financial data, operational data, employee data, customer data or intellectual property.
- Intelligence processes in place to understand the threat to the company’s assets, including their overseas operations.
- A way of identifying and agreeing the level of risk of cyber attack that the company is prepared to tolerate for a given information asset.
- Controls in place to prepare, protect, detect and respond to a cyber attack – including the management of the consequences of a cyber security incident.
- A means of monitoring the effectiveness of their cyber security controls, including where appropriate, independently testing, reviewing and assuring such controls.
- A programme of continuous improvement, or where needed, transformation, to match the changing cyber threat – with appropriate performance indicators.

³ “China Data”, KPMG, 13 June 2023

⁴ “Privacy Commissioner’s Office Recommends Organisations to Strengthen Data Security Measures to Ensure Data Security”, PCPD, 22 September 2023



Define the audit committee's oversight responsibilities for generative AI.

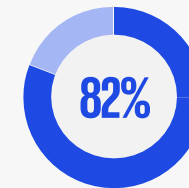
As discussed in [On the 2024 board agenda](#), oversight of generative AI will be an oversight priority for almost every board in 2024. Many boards are considering how to oversee generative AI at the full-board and committee levels.

The audit committee may end up overseeing compliance with the patchwork of differing laws and regulations governing generative AI, as well as the development and maintenance of related internal controls and disclosure controls and procedures. Some audit committees may have broader oversight responsibilities for generative AI, including oversight of various aspects of the company's governance structure for the development and use of the technology. How and when is a generative AI system or model—including a third-party model—developed and deployed, and who makes that decision? What generative AI risk management framework is used? Does the organisation have the necessary generative AI-related talent and resources?

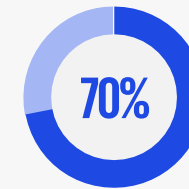
Given how fluid the situation is—with generative AI gaining rapid momentum—the allocation of oversight responsibilities to the audit committee may need to be revisited.



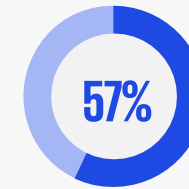
KPMG 2023 CEO Outlook findings



express concern that AI may provide new attack strategies for adversaries



consider generative AI as their top investment priority



believes ethical challenges are the number one concern when it comes to implementing generative AI

Source: "2023 China CEO Outlook", KPMG, October 2023



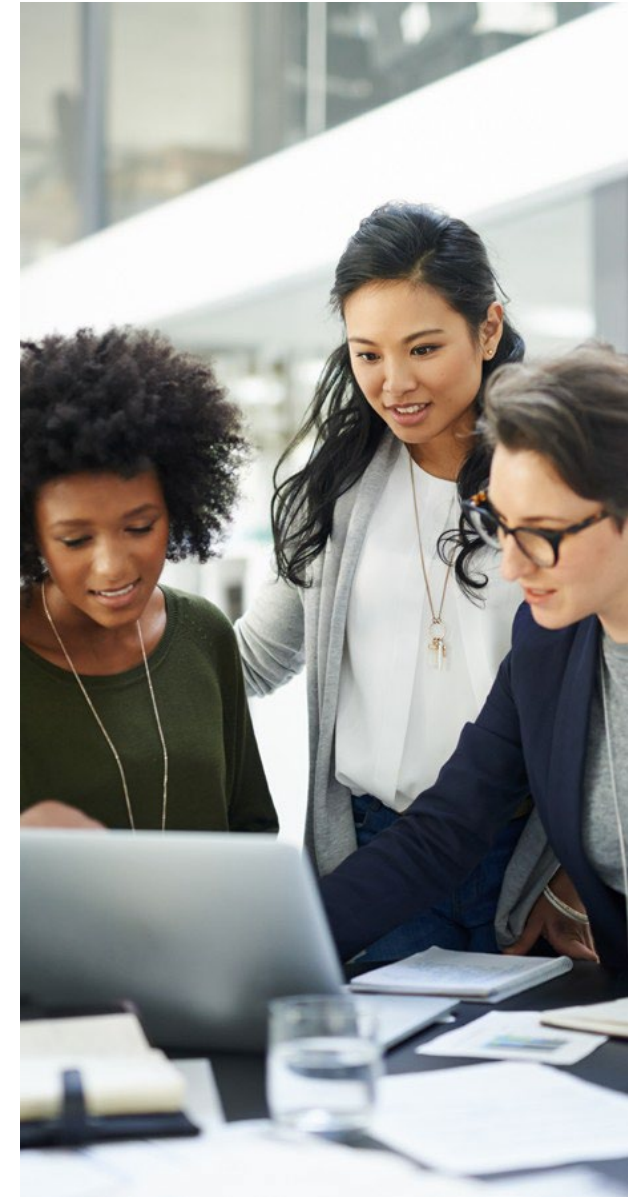
Focus on leadership and talent in the finance organisation.

Finance organisations face a challenging environment—addressing talent shortages, while at the same time managing digital strategies and transformations and developing robust systems and procedures to collect and maintain high-quality climate and sustainability data both to meet investor and other stakeholder demands and in preparation for disclosure requirements. At the same time many are contending with difficulties in forecasting and planning for an uncertain environment.

As a audit committees monitor and help guide finance’s progress in these areas, we suggest two areas of focus:

- Finance organisations can assemble or expand management teams or committees charged with managing a range of climate and other sustainability activities, and prepare for related disclosure rules—e.g., identifying and recruiting climate and sustainability talent and expertise, developing internal controls and disclosure controls and procedures, and putting in place technology, processes, and systems.
- At the same time, the acceleration of digital strategies and transformations presents opportunities for finance to add greater value to the business. The finance function is combining strong analytics and strategic capabilities with traditional financial reporting, accounting, and auditing skills.

The audit committee can devote adequate time to understanding finance’s climate/ sustainability strategy and digital transformation strategy (if there is any) and the execution progress of those strategies, as well as its existing responsibilities. Staffing deficiencies in the finance department may pose the risk of an internal control deficiency, including a material weakness.





Reinforce audit quality and stay abreast of the increasing expectations of the AFRC.

Audit quality is enhanced by a fully engaged audit committee that sets the tone and clear expectations for the external auditor and monitors auditor performance rigorously through frequent, quality communications and a robust performance assessment.

In setting expectations for 2024, audit committees should discuss with the auditor how the company’s financial reporting and related internal control risks have changed in light of the geopolitical, macroeconomic, regulatory and risk landscape, as well as **changes in the business**.

Set clear expectations for more frequent communication with auditors, fostering a culture of open and candid communications between the auditor and the audit committee, beyond what’s required. The list of required communications is extensive and includes matters about the auditor’s independence as well as matters related to the planning and results of the audit.

Taking the conversation beyond what’s required can enhance the audit committee’s oversight, particularly regarding the company’s culture, tone at the top, and the quality of talent in the finance organisation.

The Accounting and Financial Reporting Council (AFRC), as the independent audit regulator in Hong Kong, has stated that audit committees have a **critical role** in ensuring that their companies are well governed with effective internal controls that support the preparation of quality financial information. This in turn, provides a sound foundation for a high-quality audit. Therefore, staying informed of the AFRC’s current focus areas and concerns as well as their expectations of Audit Committees will improve the effectiveness of oversight.

The AFRC issues various guidelines, periodic reports and alerts to enhance and improve the quality of corporate reporting and thus, protect

public interest. For example, on 13 July 2023, the Securities and Futures Commission (SFC) and the AFRC released a joint statement in relation to loans, advances, prepayments and similar arrangements made by listed issuers, emphasising the responsibility of those charged with the governance of a company, including the audit committee, to oversee the activities of management and ensure that adequate internal control policies and procedures are established and operate effectively⁵.

In September 2023, the AFRC released two important documents: “AFRC Addresses Concerns Surrounding Auditor Changes” (“the Paper”) and the “Guidance Notes on Change of Auditors” (“the Guidance Notes”). These urge the audit committees of listed companies to remain vigilant about the remaining issues raised in the Paper and to follow the Guidance Notes so as to uphold audit quality⁶.

In October 2023, the AFRC, in collaboration with the ICAC and the SFC, carried out its first tripartite joint operation. This operation targeted two listed companies suspected of engaging in falsified corporate transactions and involved searches across more than 15 premises in Hong Kong. Subsequently, in December 2023, the AFRC issued “Audit Focus,” a publication underscoring the critical need for auditors to remain vigilant concerning the financial and audit challenges that may emerge due to the worsening economic conditions and the performance of listed companies. It sets the expectation for auditors to enhance the quality of their year-end audits by applying increased professional skepticism, particularly in key risk areas, including revenue recognition, impairment assessment, fair value measurement of assets or financial instruments, provision for onerous contracts, going concern assessment and fraud risk assessment⁷.

⁵ “Joint statement of the Securities and Futures Commission (SFC) and the Accounting and Financial Reporting Council (AFRC) in relation to loans, advances, prepayments and similar arrangements made by listed issuers”, SFC and AFRC, 13 July 2023

⁶ “AFRC urges auditors and audit committees to follow Guidance Notes on Change of Auditors”, AFRC, 28 September 2023

⁷ “Audit Focus for 2023 year-end audit”, AFRC, 22 December 2023



Make sure internal audit is focused on the company's key risks—beyond financial reporting and compliance—and is a valued resource to the audit committee.

As audit committees wrestle with heavy agendas—and risk management is put to the test—internal audit should be a valuable resource for the audit committee and a crucial voice on risk and control matters. This means not just focusing on financial reporting and compliance risks, but also critical operational and technology risks and related controls, as well as ESG risks.

ESG-related risks are rapidly evolving and include human capital management—from diversity, equity, and inclusion (DEI) to talent, leadership, and corporate culture—as well as climate, cybersecurity, data governance and data privacy, and risks associated with ESG disclosures. Disclosure controls and procedures and internal controls should be a key area of internal audit focus. Clarify internal audit's role in connection with ESG risks and enterprise risk management more generally—which is not to manage risk, but to provide added assurance regarding the adequacy of risk management processes. Do management teams have the necessary resources and skill sets to execute new climate and ESG initiatives?

Reassess whether the internal audit plan is risk based and flexible enough to adjust to changing business and risk conditions. The audit committee should work with the chief audit executive and chief risk officer to help identify the risks that pose the greatest threat to the company's reputation, strategy, and operations, and to help ensure that internal audit is focused on these key risks and related controls. These may include industry-specific, mission-critical, and regulatory risks, economic and geopolitical risks, the impact of climate change on the business, cybersecurity and data privacy, risks posed by generative AI and digital technologies, talent management and retention, hybrid work and organisational culture, supply chain and third-party risks, and the adequacy of business continuity and crisis management plans.

Given internal audit's broadening mandate, it will likely require upskilling. Set clear expectations and help ensure that internal audit has the talent, resources, skills, and expertise to succeed—and help the chief audit executive think through the impact of digital technologies on internal audit.



Work with the chief audit executive and chief risk officer to help identify the risks that pose the greatest threat to the company's reputation, strategy, and operations, and to help ensure that internal audit is focused on these key risks and related controls.



Help sharpen the company's focus on ethics, compliance, and culture.

The reputational costs of an ethics or compliance failure are higher than ever, particularly given increased fraud risk, pressures on management to meet financial targets, and increased vulnerability to cyberattacks. Fundamental to an effective compliance program is the right tone at the top and culture throughout the organisation, including commitment to its stated values, ethics, and legal and regulatory compliance. This is particularly true in a complex business environment as companies move quickly to innovate and capitalise on opportunities in new markets, leverage new technologies and data, and engage with more vendors and third parties across complex supply chains.



Closely monitor the tone at the top and culture throughout the organisation with a sharp focus on behaviors (not just results) and yellow flags. Is senior management sensitive to ongoing pressures on employees (both in the office and at home), employee health and safety, productivity, and employee engagement and morale? Leadership, communication, understanding, and compassion are essential. Does the company's culture make it safe for people to do the right thing? It is helpful for directors to spend time in the field meeting employees to get a better feel for the culture. Help ensure that the company's regulatory compliance and monitoring programs are up to date, cover all vendors in the global supply chain, and communicate the company's expectations for high ethical standards.

Focus on the effectiveness of the company's whistleblower reporting channels (including whether complaints are being submitted) and investigation processes. Does the audit committee see all whistleblower complaints? If not, what is the process to filter complaints that are ultimately reported to the audit committee? With the radical transparency enabled by social media, the company's culture and values, commitment to integrity and legal compliance, and its brand reputation are on full display.

Leadership, communication, understanding, and compassion are essential.

About the KPMG Board Leadership Center

The KPMG Board Leadership Center (BLC) champions outstanding corporate governance to drive long-term value and enhance stakeholder confidence. Through an array of insights, perspectives, and programs, the BLC—which includes the KPMG Audit Committee Institute and close collaboration with other leading director organisations—promotes continuous education and improvement of public and private company governance. BLC engages with directors and business leaders on the critical issues driving board agendas—from strategy, risk, talent, and ESG to data governance, audit quality, proxy trends, and more. Learn more at kpmg.com/cn/boardleadership

About the KPMG Audit Committee Institute

As part of the KPMG Board Leadership Center, the ACI provides audit committee and board members with practical insights, resources, and peer-exchange opportunities focused on strengthening oversight of financial reporting and audit quality, and the array of challenges facing boards and businesses today—from risk management and emerging technologies to strategy, talent, and global compliance. Learn more about ACI at <https://kpmg.com/cn/en/home/misc/board-leadership/audit-committee-institute.html>

Contact us

Shanghai:

Frank Mei
Partner

Tel: + 86 (10) 8508 7188
frank.mei@kpmg.com

Kevin Huang
Partner

Tel: +86 (21) 2212 2159
kevin.huang@kpmg.com

Joyce Ge
Partner

Tel: + 86 (21) 2212 3295
joyce.ge@kpmg.com

Stephanie Chew
Partner

Tel: + 86 (21) 2212 3080
stephanie.chew@kpmg.com

Ivy Ye
Director

Tel: + 86 (21) 2212 3327
iv.ye@kpmg.com

Effeir Li
Director

+ 86 (21) 2212 2347
effeir.li@kpmg.com

Beijing:

Charles Wan
Partner

Tel: + 86 (10) 8508 5303
charles.wan@kpmg.com

Thomas Chan
Partner

Tel: + 86 (10) 8508 7014
thomas.chan@kpmg.com

Johnson Li
Partner

Tel: + 86 (10) 8508 5975
johnson.li@kpmg.com

Vera Li
Partner

Tel: + 86 (10) 8508 5870
vd.li@kpmg.com

Haoyu Liu
Partner

Tel: + 86 (10) 8553 3343
haoyu.liu@kpmg.com

Medivh Luo
Director

Tel: + 86 (10) 8508 5016
medivh.luo@kpmg.com

Aaron Ren
Director

Tel: + 86 (10) 8508 5454
aaron.ren@kpmg.com

May Gao
Director

Tel: + 86 (10) 8508 5390
may.gao@kpmg.com

Hong Kong SAR:

Ivy Cheung
Partner

Tel: + 852 2978 8136
ivy.cheung@kpmg.com

Tom Jenkins
Partner

Tel: + 852 2143 8570
tom.jenkins@kpmg.com

Alva Lee
Partner

Tel: + 852 2143 8764
alva.lee@kpmg.com

Jia Ning Song
Partner

Tel: + 852 2978 8101
jianing.n.song@kpmg.com

Edna Wong
Partner

Tel: + 852 2143 8693
edna.wong@kpmg.com

Jens Kessler
Partner

Tel: + 852 2143 8584
jens.kessler@kpmg.com

Loo, Longhui
Director

Tel: + 852 3927 4647
longhui.loo@kpmg.com

Guangzhou/Shenzhen:

Ming Chung
Partner

Tel: + 86 (20) 3813 8828
ming.chung@kpmg.com

Kelvin Leung
Partner

Tel: + 86 (755) 2547 3338
kelvin.oc.leung@kpmg.com

Eric Chang
Partner

Tel: + 86 (20) 3813 7088
eric.chang@kpmg.com

Joyce Xie
Partner

Tel: + 86 (755) 2547 1261
joyce.xie@kpmg.com

Mona He
Director

Tel: + 86 (20) 3813 8239
mona.he@kpmg.com

Some or all of the services described herein may not be permissible for KPMG audit clients and their affiliates or related entities.



kpmg.com/cn/socialmedia

The information contained herein is of a general nature and is not intended to address the circumstances of any particular individual or entity. Although we endeavor to provide accurate and timely information, there can be no guarantee that such information is accurate as of the date it is received or that it will continue to be accurate in the future. No one should act on such information without appropriate professional advice after a thorough examination of the particular situation.

© 2024 KPMG Advisory (Hong Kong) Limited, a Hong Kong (SAR) limited liability company and a member firm of the KPMG global organisation of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved. Printed in Hong Kong (SAR).

The KPMG name and logo are trademarks used under license by the independent member firms of the KPMG global organisation.